WHAT IS CLAIMED IS:

1. A method of sending a packet from a first IPSec client to a second IPSec client, comprising the steps of:

receiving at a non-proprietary format tunneling protocol server from the first IPsec client an IPsec packet wrapped in the non-proprietary tunneling format;

creating a non-proprietary format tunneling protocol tunnel to the second IPsec client through the non-proprietary format tunneling protocol server;

establishing a security association between the first and second IPSec clients via the non-proprietary format tunneling protocol server;

transmitting the packet through the non-proprietary format tunneling protocol tunnel to the second IPSec client whereby the packet remains unaffected by any address translation or firewall traversal that may occur during transmission.

2. The method according to claim 1 wherein the non-proprietary tunneling protocol comprises a Layer-2 Tunneling Protocol (L2TP) protocol.

3. The method according to claim 2 wherein the receiving step includes the steps of:

opening an LT2P tunnel between the first IP client and the server; and

communicating an IPsec packet wrapped in an L2TP format to the server.

4. The method according to claim 2 wherein the receiving step includes the step of routing an IPsec packet wrapped in an L2TP format to the server via a public address.

5. The method according 4 wherein the public address supplied from the server to the first IPsec client.